CONTRACT FOR

SECURE DESTRUCTION SERVICES

Contract # 050815-A-CCG-DD

1.0 INTRODUCTION:

This agreement is entered into by the Council on Competitive Government (CCG), the Texas State Library and Archives Commission (TSLAC), TIBH Industries, Inc. (TIBH) and its' Community Rehabilitation Programs (CRPs) and will be known as the Secure Destruction Services Contract. Through this Contract, CCG and TSLAC seek to acquire Secure Destruction Services that:

- prevent the disclosure of state records and personal information
- provide the best value to Texas state agencies, state universities, local governments, non-profits, and co-op participants
- can be utilized across the entire State
- are characterized as "non-mobile" and are performed away from the Participating Agency's premises.

CRPs that meet the criteria specified in Sections 3.1 and 3.2 below are eligible to provide services under the resulting Secure Destruction Services Contract. TIBH will be responsible for managing this Contract and for coordination among CRPs as the Certifying Party. TIBH will make reasonable efforts to see that Secure Destruction Services are available to Participating Agencies (PAs) across the State.

PAs should be aware that the services under this Contract are offered in accordance with Texas Government Code 2162 as well as Texas Human Resources Code Chap. 122, particularly Sections 122.007 (*Fair Market Price; Purchasing Procedures*) and 122.008 (*Procurement at Determined Price*).

2.0 DEFINITIONS:

When capitalized, the following terms have the meaning set forth below. All other terms have the meaning set forth in the *dictionary name*.

45-Day Notification: Under IRS Pub. 1075, a PA that seeks to release Federal Tax Information to a contractor must notify the IRS at least 45 days prior to the release.

Alarm System: An electronic system capable of detecting and alerting the user to specific dangers including: intrusion and fire.

Business Days: The period of time from 7:00 a.m. to 6:00 p.m. exclusive of weekends and observed holidays when the offices of a non-CRP's (e.g. PA, TIBH, CCG, TSLAC) are open. See also CRP Business Days.

Business Hours: CRP's regularly scheduled hours of operation. See also Non-Business Hours.

CCG: The Council on Competitive Government

Contract: This Contract for Secure Destruction Services.

CRP: Community Rehabilitation Program

CRP Business Days: The period of time, typically 8:00 a.m. to 5:00 p.m. and exclusive of weekends and observed holidays, when the CRP's offices are open. See also Business Days.

Destroy or Destroyed: The rendering of paper records and other material so that the information it contained can no longer be viewed. Materials destroyed in conformance with the appropriate standard as set forth in the applicable section of this Contract shall be presumed to meet this definition.

Document: A written or printed instrument that conveys information that is placed in a Secure Container.

Electronic Equipment: For the purposes of this Contract, includes:

- e-Waste
- Hard Drives
- Media
- Visual Display Units

e-Waste (electronic waste): Electronic devices including, but excluding Hard Drives and Media:

- computers
- computer components
- servers
- flat panel monitors
- printers
- copiers
- scanners
- wiring and cabling
- telephone switches and handsets
- projectors
- recording devices
- audio/video equipment
- cell phones

that are obsolete due to technological advances or when said device no longer works as designed.

NOTE: e-Waste does **not** include

- Hard Drives
- Media
- Visual Display Units
- Alkaline or lithium batteries
- Toner cartridges of any kind

Economically Feasible: A determination that the benefits of an action outweigh the action's costs.

FTI: Federal Tax Information

Hard Drives: Non-volatile, random access devices for storing digital data that can be found in many electronic devices including, but not limited to, computers, servers, copiers and scanners.

Hours: Clock hours.

IRS: Internal Revenue Service.

Materials: Any items to be Destroyed, including, but not limited to, Documents, e-Waste, and Non-Traditional Items, removed from a Participating Agency's premises by a CRP.

Media: Any media including, but not limited to, Microfilm, Microfiche, CDs, Floppy Disks, Data Tapes, Cassette Tapes, VHS Tapes, film and/or data stored on

reel-to-reel tapes that contains confidential information and must be protected and Destroyed with similar safeguards as Documents.

Minimum Trip Charge: The minimum amount a CRP needs to cover the expense of making a trip to a specific location. Examples of costs that may be included in a Minimum Trip Charge include (but are not limited to): the cost of fuel and the cost of labor.

NAID: National Association for Information Destruction

NAID Certification (*AAA Certification, Certification Program*): Words used interchangeably throughout the NAID Certification Program information referring to NAID Certification or to identify a facility or company that meets all NAID standards regarding security and other operational characteristics.

Non-Business Hours: CRP's regularly schedule hours of non-operation.

Non-Traditional Items: Items, other than paper, plastic, or e-Waste, requiring destruction and/or recycling due to the presence of logos, expired program or benefit information and/or other PA identifying information.

Participating Agency (PA): State agencies, state universities, local governments, non-profits, or local co-op entities in Texas that are required or permitted by law to purchase goods and services under contracts established by the CCG (Texas Government Code 2162) or TCPPD (Texas Human Resource Code 122).

Private Vendor: A "for-profit", non-CRP vendor.

Secure: Administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Secure Container: A locked bin or receptacle, into which Documents are placed. Under some circumstances and as agreed to between PA and CRP, boxes or other bulk packages (e.g. boxes palletized and shrink wrapped) may be included in this definition.

Security Monitoring System: An electronic system capable of monitoring, capturing, and storing information on physical activities (i.e. a video monitoring system).

Standard Fee Schedule: A listing of fees for services negotiated periodically between a PA, a CRP, and TIBH that is submitted to TCPPD for review and approval.

Subcontractor: Any entity the CRP uses to provide services that are an integral part of the CRP's destruction service program and whose employees or agents have access to confidential customer media to be Destroyed, such as providers of temporary staffing, transportation.

TCPPD: Texas Council on Purchasing from People with Disabilities. TCPPD determines the fair market price of services offered under this Contract (Texas Human Resource Code 122.007).

TIBH: TIBH Industries, Inc.

TSLAC: Texas State Library and Archives Commission

Visual Display Unit: A device for viewing electronic data including cathode ray tubes (CRTs), television monitors, computer displays, etc., but does not include flat panels.

Zero Landfill Impact: The amount of material sent to a landfill is minimal or none.

3.0 MINIMUM CRP REQUIREMENTS:

All CRPs that wish to participate in the Contract must meet or comply with the requirements within this section.

3.1 General Requirements

3.1.1 NAID Certification

All CRPs and their Subcontractors must have and maintain a current NAID AAA certification in order to provide services under this Contract. For NAID AAA certification details see:

http://www.naidonline.org/nitl/en/cert/documents.html

3.1.1.1 Notification of Change in NAID Status

Upon any change in NAID AAA status, including the loss of certification or any audit finding that could result in loss of certification, while providing services under this Contract, CRP must notify TIBH within three (3) Business Hours of the change in status. Notification must be provided via e-mail.

3.1.1.2 Loss of NAID Certification

Should CRP lose NAID AAA certification while providing services under this Contract, the CRP must:

- Notify TIBH as set forth in Section 3.1.1.1
- Cease receiving or collecting Materials from PAs by no later than close of business on the day CRP is notified of its loss of certification
- Work with TIBH, PAs, and alternate CRPs or destruction vendors to see that:
    - Any remaining PA Materials are Destroyed in accordance with the standards set forth in this Contract
    - The provision of services is transferred to another vendor (CRP or Private Vendor) with the timeframes and under the conditions negotiated with TIBH and/or PAs.

3.1.2 Compliance with Destruction Standards

CRP must Destroy all Materials according to appropriate government (federal and state) standards as well as any standards established under this Contract (See: Sec. 3.2.2; Sec. 4.1.1; and Sec. 4.2.1). Appropriate government standards may include but are not limited to:

- IRS Publication 1075
- HIPAA Privacy Rules (45 CFR 164.530(c))
- Internal Revenue Manual (IRM) 1.15.3
- Texas Government Code 441.180-189
- Texas Local Government Code 202.003
- 13 Texas Administrative Code Chapters 6 or 7

Compliance with this section will also include participation in Business Associate Agreements (BAAs) as they relate to the Health Insurance Portability and Privacy Act of 1996. A sample of a BAA is attached to this agreement (see Attachment 1).

3.1.3 Federal Requirements and Certifications

3.1.3.1 Receipt of Federal Tax Information (FTI)

Any CRP who receives FTI from a PA is deemed to have accepted, and agreed to, the provision in Exhibit 7 of IRS Publication 1075 attached to, and expressly incorporated, herein (see Attachment 2 of this Contract) CRP's will assist PA in submitting their 45-Day Notification to the IRS including the provision of information to PA for the 45 Day Notification Letter.

3.1.3.1.1 Denial of Service – 45 Day Notification Letter
A CRP may withhold service to a PA until the PA has received approval from the IRS under the 45-Day Notification Requirements.

3.1.3.1.2 IRS Approval of Disclosures to Subcontractors
CRPs must notify and secure the approval of the IRS prior to releasing FTI to any Subcontractor. (See Attachment 3 for additional details).

3.1.3.2 Additional Federal and State Requirements

CRPs shall agree to all terms, conditions and/or certifications a PA may require due to state or federal law, and shall execute all necessary additional documents associated with same.

3.1.3.3 Failure to Agree to Terms

If a CRP is unable to agree to all terms, conditions and/or certifications and execute all additional documents required by a PA due to state or federal law, CRP must notify TIBH within one (1) CRP Business Day. See also Sec. 5.5 of this Contract.

3.1.4 Responsibility for Security

CRP must Secure all Materials from the time of pickup from PA until it has been disposed of according to specifications within this Contract.

3.1.5 Secure until Destruction

CRP must not use, allow access to, or offer for resale or use any Materials or the information contained therein until it has been Destroyed.

3.1.6 Destruction within Three (3) CRP Business Days

CRP must Destroy all Materials within three (3) CRP Business Days from the time of pickup from PA.

3.1.7 Waiver for Destruction beyond Three (3) CRP Business Days

Destruction of any Materials may only occur later than three (3) CRP Business Days after pickup from the PA's premises if the PA provides a written waiver for later destruction.

3.1.8 Facility Requirements

All of the facility requirements in Section 3.1.7 are applicable to collection, storage, and destruction facilities.

3.1.8.1 Security

3.1.8.1.1 Physical Security

CRP's facilities must be equipped with standard physical security measures which include active barriers to entry such as:

- fencing around the facility
- secure dock doors
- single entry points

3.1.8.1.2 Physical Security Protocols / Procedures

Physical security protocols must be active from the time Materials are delivered / received until the time all Materials have been Destroyed.

3.1.8.1.3 Alarm Systems

CRP's facilities must be equipped with Alarm Systems. Alarm Systems must be monitored by a third party vendor with clear protocols for whom to contact and when the local authorities are to be dispatched to the site for inspection.

3.1.8.1.4 Security Monitoring Systems

CRP's facilities must be equipped with Security Monitoring Systems.

3.1.8.1.5 Activation of Alarm and Security Monitoring Systems

At a minimum, Alarm Systems and Security Monitoring Systems must be activated during Non-Business Hours and proof of regular testing of said systems shall be available upon request.

3.1.8.3 Restrictions on Visitors

At a minimum, the CRP must follow the guidelines and protocols established under their NAID Certification in regard to allowing visitors into the areas that contain Materials prior to being Destroyed.

CRP must get a signed confidentiality agreement from all visitors.

3.1.8.4 Restrictions on devices

CRP must not allow an employee or a visitor to bring cell phones, smart phones, cameras, or any other recording or transmission devices into destruction areas or areas that contain Materials prior to being Destroyed.

3.1.9 Personnel

CRP must ensure all personnel handling the Documents have undergone and passed a background check to be able to handle secure Materials as required by NAID AAA Certification standards.

CRP must get a signed confidentiality agreement from all personnel.

3.1.10 Training of CRP Employees

CRP must provide comprehensive, in-service training to their employees regarding the handling of Materials.

3.1.11 Training to PAs

CRP's training for PAs must, upon request and at a minimum, cover liability as well as the proper types of Documents or Materials to place in Secure Containers and pickup areas.

3.1.12 Scheduling with PAs

3.1.12.1 Establishing Pick-Ups

CRP is responsible for working with PA to establish pick up times, and any policies and procedures necessary to prevent conflict with the provisions of this Contract.

3.1.12.2 Work Order Documentation

The CRP will document all pickups of containers, boxes or other by issuing a descriptive work order, with unique work order number, that will be signed and dated by CRP personnel and PA's personnel at the time of pickup. Description must include name of PA, name of PA's point of contact as well as their e-mail address and/or phone number, location of pickup, date of pickup, quantity and name of item(s) being picked up from the PA. Information on the work order will be consolidated to appear on the invoice.

The work order will act as proof of the transfer of material into the possession of the CRP and will be used to support the invoice. The PA may request a copy of a work order at any time. Any pickup not substantiated by a signed work order may be deducted from the invoice by the PA.

3.1.12.3 Responsibility for Pick-Ups

CRP will pick up Secure Containers or boxes on pallets from each PA at an agreed to time and date.

3.1.12.4 Deviations from Schedule

CRP will schedule regular pickups and shall not deviate from the stated schedule without prior approval from the PA unless state or national holidays or force majeure prevent it from doing so. CRP is to negotiate a resolution with a PA in the instance where the CRP fails to meet the established schedule.

In the event that PA and CRP are unable to negotiate a resolution, CRP must notify TIBH within one (1) CRP Business Day.

See also Sec. 5.5 of this Contract.

3.1.13 Invoicing

CRP must provide a detailed invoice to PA via TIBH on a monthly basis for services provided during the previous month. Payment will be made to TIBH as assignee.

3.1.14 Certificates of Destruction

CRP must provide PA with certificates of destruction for all Materials Destroyed under the Contract. Certificates of destruction will be included with each month's invoice.

3.1.15 Option to Increase or Decrease Quantities

A PA, at its' sole discretion, may increase or decrease the number of locations, the number of Secure Containers, or the number of pickups at the same unit prices agreed upon in the Contract. Any change in quantities of locations, will be processed via a Purchase Order Change Notice prior to increasing or decreasing quantities.

3.1.16 Approval of Prices and Price Changes

Before participating on this Contract, CRP must submit a complete list of all prices they will charge under the Contract to Texas Council on Purchasing from People with Disabilities (TCPPD) for review and approval. Similarly, any change in a CRP's prices under this Contract must be reviewed and approved by TCPPD prior to implementation.

3.1.17 Notification of PAs of Prices and Price Changes

CRP must provide or make available an approved (see Sec. 3.1.16) pricing sheet to PAs. CRP must provide thirty (30) calendar days notification prior to the submission of a price change request to TCPPD. CRP must also provide thirty (30) calendar days notice to PAs of any price change approved by TCPPD.

3.2 Document Destruction Requirements

3.2.1 Secure Containers, Vehicles, and Facilities

CRP will enclose Documents already contained in a Secure Container within a securely enclosed vehicle at the time of removal to CRP's offsite destruction facility. Any boxes of Documents should be transported on pallets and shrink-wrapped. Boxes may be loaded into Secure Containers before removal from PA location.

3.2.2 Document Destruction Standard

CRP will Destroy Documents by shredding to 5/8 of an inch or smaller as specified by the PA.

Note: If any other method is proposed, the proposal shall describe the method in detail. The proposed method is subject to the approval of the PA and TSLAC.

3.2.3 Post-Shredding

CRP must ensure that Documents described under the Contract shall only be sold directly to a domestic paper mill and receive an additional certificate of destruction from the paper mill. The certificate of destruction provided by the paper mill shall be made available to the PA or TSLAC upon request.

4.0 OPTIONAL CRP REQUIREMENTS

CRPs that wish to offer Electronic Equipment Destruction Services under this contact must meet or comply with the requirements of Section 4.1.

CRPs that wish to offer Non-Traditional Items Destruction Services under this Contract must meet or comply with the requirements of Section 4.2.

4.1 Electronic Equipment Destruction Requirements

4.1.1 Electronic Equipment Destruction

CRP must completely Destroy each Electronic Equipment item so that it can no longer be utilized in its original form or for its intended purpose.

4.1.2 Electronic Equipment Recycling

To the extent it is economically feasible, CRP must recycle Electronic Equipment such that there is zero landfill impact. All Electronic Equipment received under the resulting Contract will be Destroyed and smelted, crushed and/or shredded with the intended purpose of smelting the final product for precious metal recycling.

4.1.3 Media & Hard Drive Destruction Standard

Media and Hard Drives must be Destroyed to the degree that any information they may contain is no longer accessible or readable by any means. This destruction must be completed before the Media or Hard Drive is recycled.

4.2 Non-Traditional Item Destruction

4.2.1 Non-Traditional Items Destruction Standard

CRP must Destroy, crush and/or shred all Non-Traditional Items received from a PA with the intended purpose of making reuse in its original form or for its intended purpose impossible.

4.2.2 Recycling of Non-Traditional Items

Non-Traditional Items should be slated for destruction by PA only after it has been determined that the items cannot be recycled through the Texas Facilities Commission's recycling program. All Non-Traditional Items should be recycled to the maximum extent possible.

4.2.3 Landfill Impact

To the extent it is economically feasible, CRP should endeavor to ensure Non-Traditional Items have zero landfill impact.

5.0 TIBH REQUIREMENTS:

5.1 Statewide Coverage

TIBH will coordinate CRPs and manage this Contract so that, to the extent possible, Secure Destruction Services are available statewide.

5.2 Changes in Status of CRPs

TIBH will notify TSLAC and CCG when there is a change in the status of any CRP under the Contract.

Should a CRP lose its NAID AAA certification or cease providing services while under Contract, TIBH must notify PAs, CCG and TSLAC within two (2) Business Days. TIBH must also inform CCG and TSLAC about any and all corrective measures to address the loss of services provided by the CRP.

5.3 Reporting Requirements

TIBH will submit Contract performance reports to TSLAC and CCG. TIBH will work with TSLAC and CCG to establish the format and frequency of the reports to be submitted.

5.4 Notification of Pricing and Price Changes

TIBH will be responsible for notifying CCG and TSLAC regarding any proposed and finalized price changes under this Contract and the TCPPD process. TIBH must provide CCG and TSLAC with electronic copies of new pricing information / price sheets within five (5) Business Days of implementation.

5.5 Challenge Review and Resolution

TIBH will be responsible for reviewing and resolving any challenges that cannot be settled between a PA and a CRP. Such challenges may include:

- Failure to agree to terms (Sec. 3.1.14.3)
- Failure to agree to schedule (Sec. 3.1.11.4)

In the event TIBH is unable to negotiate a resolution between a PA and a CRP, and is unable to transition the service to another CRP thereby resolving the challenge to the satisfaction of the PA, then TIBH will grant a release to PA so that it may procure destruction services from a Private Vendor.

5.6 Oversight over Transitions

TIBH will ensure that there is an orderly transition of service whether the transition occurs between a PA and a CRP, a CRP and another CRP, or a CRP and a Private Vendor.

6.0 PARTICIPATING AGENCY RESPONSIBILITIES

6.1 Responsibility until Removal

Materials deposited in CRP-provided receptacles are the responsibility of the PA until they are removed from the premises by the CRP.

6.2 Scheduling with CRP

PAs must work with CRP in order to establish pick up times and any policies and procedures not to conflict with the provisions of this Contract.

PAs should provide CRP with a copy of their holiday calendar at the beginning of each Fiscal Year and work with CRP to establish a pick up schedule based on the calendar.

6.3 Notice of Scheduled Agency Closure - 24 hours in advance

PAs must give CRP a minimum of 24 hours advance notice of any scheduled closure that would impact a scheduled pick up.

6.4 Failure to Notify CRP of Agency Closure

In the situation where:

1. a PA fails to inform a CRP (see "Notice of Agency Closure" above) that it will be closed (whether scheduled or emergency) on the date of a scheduled pick-up; AND
2. the CRP attempts the pick-up at the PA's facility on the scheduled date;

the CRP may invoice the PA for a Minimum Trip Charge (see applicable fee schedule) for the missed scheduled pickup.

6.5 Payments to TIBH

PA will be responsible for remitting payments for services to TIBH.

6.6 Electronic Equipment Preparation

PA should have Electronic Equipment palletized and ready for removal prior to removal by the CRP. Otherwise, CRPs may:

- charge additional fees to prepare; or
- refuse to remove the Electronic Equipment.

CRPs may also charge an additional fee if the removal of Electronic Equipment involves emptying a warehouse or office. See applicable CRP fee schedule for details.

6.7 Purchase Order Requirements

All Purchase Orders must be made out to TIBH Industries, Inc. and include:

- Dates of service (fiscal year, month, or arranged one-time pick-up date)
- Listing of specific locations (any addresses for the pickup(s))
- Contact information (for pick-up locations and requesting parties, if different)
- Billing address and contact
- Number and size of receptacles (quantity and size of boxes, bins, etc.)
- Material type (paper, microfilm, etc.)
- Service type and frequency (weekly, every 2 weeks, every 4 weeks, one-time pick-up)
- CCG Contract #050815-A-CCG-DD
- Total dollar amount
- Authorized signature

6.8 Release of Federal Tax Information (FTI) & 45-Day Notification to IRS

PAs that release FTI to CRPs under this Contract must submit a 45-Day Notification Letter to the IRS prior to releasing FTI to a CRP. See Attachment 3of this Contract or Exhibit 12 of IRS Pub. 1075.

6.9 Responsibility for Damaged or Lost Containers

PA will be responsible for compensating CRP for a container that is either lost or damaged to the point that it can no longer safely or effectively be used for its designated purpose. Compensation will be due to the CRP if the loss or damage to the container was sustained while it was under the control of the PA. Any compensation paid to the CRP must not exceed the cost to replace a lost or damaged container.

7.0 FEES:

7.1 Establishment of Fee Schedule

Each CRP under this agreement must establish and adhere to a Standard Fee Schedule for the area which it serves.

7.2 No Fee for Storage due to Delayed Destruction

CRP will not charge additional fees (e.g., a fee for storage) for Materials that cannot be Destroyed within three (3) CRP Business Days.

7.3 Fees for Pick-ups when PA is closed

See "Failure to Notify CRP of Scheduled Agency Closure" (Section 7.4) above.

8.0 TERMS AND CONDITIONS:

8.1 Contract Term and Renewals

The provisions of this agreement shall become effective on September 1, 2012 or on a prior date as established between a PA and the CRP and shall terminate on August 31, 2020, unless otherwise sooner terminated as provided by this agreement. Upon expiration of the initial Contract term, the Contract may be renewed for additional term in any combination of years or months at the discretion of CCG.

8.2 Termination for Convenience

CCG may, at its sole discretion, terminate this agreement upon written notice to TIBH. Such notice may be provided by facsimile or certified mail, return receipt requested, and is effective thirty (30) calendar days after receipt of notification by TIBH. TIBH or a CRP may terminate the services by providing no less than 60 days notice of such intent to terminate, and receiving permission from TCPPD to terminate in a public meeting.

Upon receipt of termination notification, TIBH will work with PA's to ensure an orderly transition between CRPs or to move the work to other destruction services providers for all PAs with open Purchase Orders, work orders as well as work in process.

9.0 SIGNATURES:

State Council on Competitive Government

By: 

(Printed Name)

MIKE MORRISSEY

(Title) SR. ADVISOR

Date: 8-7-12

TIBH Industries, Inc. (TIBH)

By: Abby Mark

Abby Mark

(Printed Name)

Regional Marketing Manager

(Title)

Date: 8/2/2012

Attachment 1

SECURE DESTRUCTION SERVICES CONTRACT

Contract # 050815-A-CCG-DD

kip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

lealth Information Privacy

3usiness Associate Contracts

;AMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS[1]
Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only addres concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contrac under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions[2]

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

a. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].
b. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].
c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

e. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103.
g. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Busines Associate with respect to such information.
f. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.
g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]
h. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
j. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

ermitted Uses and Disclosures by Business Associate

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use o disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:
[List Purposes].

b. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information fo the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
c. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).
d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that suc restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]
b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
    1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
    2. Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or
    3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

    [Bracketed language in this provision may be necessary if there is an underlying services agreement Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.
    1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
    2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

ıealth Information Privacy

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
c. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.
d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

[1] This website version of Sample Business Associate Contract Provisions was revised June 12, 2006 to amend th ·egulatory cites to the following terms: "individual"; "protected health information"; and "required by law."

[2] Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

Back to Top

Attachment 2

SECURE DESTRUCTION SERVICES CONTRACT

Contract # 050815-A-CCG-DD

The agency should include the Exhibit 7 language for either General Services or Technology Services, as appropriate and include the language below to the greatest extent possible, applicable to the specific situation.

CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(6) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(7) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of

unauthorized disclosure. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS:

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Attachment 3

SECURE DESTRUCTION SERVICES CONTRACT

Contract # 050815-A-CCG-DD

Procedures for 45-day Notification of contractor access to FTI

Federal agencies, state tax agencies, and state child support enforcement agencies in the possession of FTI may use contractors, sometimes in limited circumstances. Human Services agencies may not provide FTI access to contractors. Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor, or at least 45 days prior to the disclosure of FTI, to ensure appropriate contractual language is included and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors.

To provide agency notification of intent to enter into an agreement to make disclosures of FTI to a contractor, submit a letter in electronic format, on agency letterhead over the head of agency's signature, to SafeguardReports@IRS.gov. Ensure the letter contains the following specific information:

- Name, address, phone number and email address of agency point of contact
- Name and address of contractor
- Contract number and date awarded
- Period contract covers, e.g. 2003-2008
- Type of service covered by the contract
- Number of contracted workers
- Name and description of agency program contractor will support
- Detailed description of the FTI to be disclosed to contractor
- Description of the work to be performed by the contractor, including phased timing, how the FTI will be accessed and how tasks may change throughout the different phases
- Procedures for agency oversight on contractor access, storage and destruction of FTI, disclosure awareness training, and incident reporting
- Location where work will be performed (contractor site or agency location) and how data will be secured if it is moved from the secure agency location
- Statement whether subcontractor(s) will have access to FTI
- Name(s) and address(es) of all subcontractor(s), if applicable
- Description of the FTI to be disclosed to the subcontractor(s)
- Description of the work to be performed by subcontractor(s)
- Location(s) where work will be performed by subcontractor(s) and how data will be secured if it is moved from a secure agency location
- Certification that contractor personnel accessing FTI and contractor information systems containing FTI are all located within the United States or territories as FTI is not allowed off-shore.

After receipt of an agency's request, the IRS will analyze the information provided to ensure the contractor access is authorized and consistent with all requirements, then IRS will send the agency a written acknowledgement, along with a reminder of the requirements associated with the contract. Agency disclosure personnel may wish to discuss local procedures with their procurement colleagues to ensure they are part of

the contract review process and the appropriate contract language is included from the beginning of the contract.

If the 45-day notification pertains to the use of contractors in conducting tax modeling, revenue estimation or other statistical purposes utilizing FTI, the agency must also submit a separate statement detailing the methodology and data to be used by the contractor. The Office of Safeguards will forward the methodology and data statement to the IRS Statistics of Income office for approval of the methodology. (see section 11.3)